IMPLEMENTASI DIFFIE-HELLMAN, AES-128 DAN ECDSA PADA APLIKASI *INSTANT MESSAGING*

SKRIPSI

Diajukan untuk memenuhi bagian dari syarat memperoleh gelar sarjana pada program Studi Ilmu Komputer

Oleh:

Ammar Ashshiddiqi

NIM: 1600095

DEPARTEMEN PENDIDIKAN ILMU KOMPUTER

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2021

IMPLEMENTASI DIFFIE-HELLMAN, AES-128 DAN ECDSA PADA APLIKASI *INSTANT MESSAGING*

Oleh

Ammar Ashshiddiqi

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Pendidikan pada Fakultas Pendidikan Bahasa dan Seni

Universitas Pendidikan Indonesia

Januari 2021

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA DIFFIE-HELLMAN, AES-128 DAN ECDSA PADA APLIKASI *INSTANT MESSAGING*

Oleh:
Ammar Ashshiddiqi
NIM: 1600095

Disetujui dan disahkan oleh:
Pembimbing I,

Dr. Muhamad Nursalman, S.Si., M.T.
NIP. 197909292006041002.

Pembimbing II,

Rizky Rachman Judhie P., M.Kom.
NIP. 19771125200641002.

Mengetahui,
Ketua Departemen Pendidikan Ilmu Komputer,

Dr. Rani Megasari, S.Kom., M.T.
NIP. 198705242014042002

KATA PENGANTAR

Alhamdulillah, penulis panjatkan puji dan syukur kepada Allah SWT karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Diffie-Hellman, AES-128 dan ECDSA Pada Aplikasi *Instant Messaging*".

Sholawat dan salam semoga tercurah kepada Nabi Muhammad SAW, beserta keluarganya, sahabatnya, serta pengikutnya hingga akhir zaman.

Skripsi ini tidak akan selesai tanpa dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih sebesar-besarnya:

1. Bapak Dr. Muhamad Nursalman, S.Si., M.T. selaku pembimbing satu atas ilmu, bimbingan dan dukungan dalam penulisan dan penyusunan skripsi sehingga skripsi ini selesai, serta dalam penulisan dan penyusunan artikel.
2. Bapak Rizky Rachman Judhie P, M.Kom. selaku Pembimbing Akademik dan pembimbing dua atas ilmu, bimbingan dan dukungan selama penulis menempuh pendidikan dan menyelesaikan skripsi.
3. Bapak Eddy Prasetyo Nugroho, M.T. sebagai penguji atas ilmu, saran, dan masukan yang diberikan untuk perbaikan skripsi ini.
4. Bapak Herbert Siregar, M.T. sebagai penguji atas ilmu, saran, dan masukan yang diberikan untuk perbaikan skripsi ini.
5. Dr. Yudi Wibisono, M.T. atas bimbingannya dalam penyusunan artikel sebagai syarat prasidang.
6. Ibu Dr. Rani Megasari, S.Kom., M.T. selaku Ketua Program Studi Ilmu Komputer.
7. Seluruh dosen jurusan ilmu komputer atas ilmu dan bimbingannya selama penulis menempuh pendidikan.
8. Seluruh staf jurusan ilmu komputer atas dukungan dan bantuannya selama penulis menempuh pendidikan.

9. Kedua orang tua dan keluarga besar H. Kosasih atas dukungan dan do'a yang telah diberikan.
10. Teman-teman seperjuangan, M. Adnan Khairi, M. Izhar, Asep Saepul Achmad, Iqdam Musayyad, M. Faris Muzakki, Naufan Rusyda Faikar, Yahya Firdaus, Reyhan Fikri, IGN Agung AAW, Genta Satria, Teguh Aprianto dan Renra Noviana atas kerja sama, dukungan dan bantuan selama penulis menempuh pendidikan.
11. Teman-teman jurusan ilmu komputer angkatan tahun 2016.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna oleh karena itu, kritik dan saran sangat diperlukan demi perbaikan skripsi ini. Semoga skripsi ini bermanfaat, khususnya bagi penulis, umumnya bagi pembacanya.

Bandung, Januari 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Instant messaging merupakan salah satu teknologi komunikasi yang banyak digunakan masyarakat. Banyaknya pengguna *mobile instant messaging* dapat membuka peluang kejahatan, diantaranya penyabotasean pesan. Penggunaan kriptografi adalah salah satu metode yang tepat untuk menjaga keamanan data atau informasi saat berkomunikasi. Keamanan pesan dilakukan dengan menggabungkan algoritma pertukaran kunci, algoritma enkripsi simetris serta algoritma tanda tangan digital. Kombinasi algoritma Diffie-Hellman, AES-128 dan ECDSA dilakukan sebagai pengaman pesan. Algoritma Diffie-Hellman dipilih karena memiliki kelebihan dalam hal kemudahan pembuatan kunci efemeral, dan adanya autentikasi pengirim dan penerima, algoritma AES-128 dipilih karena kecepatan proses enkripsinya lebih cepat dan memakan memori paling kecil dibandingkan jenis algoritma AES lainnya, serta algoritma ECDSA dipilih untuk mengatasi serangan pada algoritma Diffie-Hellman saat pertukaran kunci karena memiliki keunggulan dalam hal waktu eksekusi dan jumlah penyimpanan yang digunakan lebih kecil. Diffie-Hellman digunakan sebagai algortima pertukaran kunci enkripsi pesan, AES-128 digunakan sebagai enkripsi pesan, dan ECDSA digunakan sebagai pengenal pengirim pesan. Algoritma AES-128, pada enkripsi pesan menghasilkan *ciphertext* dalam bentuk blok biner berukuran 128 bit, algoritma Diffie-Hellman menghasilkan *cipherkey* dalam bentuk format blok biner 128 bit, dan algoritma ECDSA menghasilkan tanda tangan digital dengan ukuran 256 bit. Dari gabungan ketiga algoritma tersebut, enkripsi pesan menghasilkan pesan berbentuk acak sehingga isi pesan asli yang dikirimkan tidak dapat dilihat oleh pihak lain selain pengirim dan penerima pesan. Pada proses dekripsi, tanda tangan digital pesan yang telah digenerasi algoritma ECDSA diverifikasi ksliannya. Selanjutnya, penerima mengambil *cipherkey* yang sebelumnya telah digenerasi dengan algoritma Diffie-Hellman dan digunakan untuk melakukan dekripsi *ciphertext* menjadi pesan sebenarnya menggunakan algoritma AES-128. Hasil menampilkan pesan asli yang dikirim oleh pengirim pesan, sehingga penerima pesan dapat mengetahui maksud pesan yang diterimanya. Proses enkripsi dengan algoritma AES-128 menunjukkan dekripsi bisa dilakukan dan pesan *ciphertext* berbentuk acak, sehingga kerahasiaan dan integritas data terjaga. Pada pengujian dengan kunci yang berbeda pada proses dekripsi tidak ada yang sesuai dengan isi *plaintext* asli, sehingga penggunaan algoritma Diffie-Hellman pada pertukaran kunci AES-128 dapat menjaga integritas data. Pengujian dengan ECDSA menunjukkan hasil validasi 100% dikirim dari pengirim asli, sehingga memenuhi autentikasi dan nir-penyangkalana. Kecepatan proses enkripsi didapat, 43540,375 bit/detik, sedangkan pada proses dekripsi didapat kecepatan 1251,705 bit/detik. Hal ini menunjukkan bahwa *throughput* dari proses dekripsi lebih lambat dibandingkan dengan *throughput* proses enkripsi.

Kata kunci: *Instant Messaging*, Kriptografi, Diffie-Hellman, AES-128, ECDSA.

DAFTAR ISTILAH

Istilah	Arti
AES	*Advanced Encryption Standard*, Algoritma kriptografi yang digunakan untuk mengenkripsi data dan merupakan standar algoritma simetris
ASCII	*American Standard Code for Information Interchange*, adalah standar pengkodean karakter untuk komunikasi elektronik
Avalanche Effect	Efek yang diukur pada *ciphertext* ketika terjadi pengubahan kecil pada teks biasa atau kuncinya
Bandwidth	Kecepatan maksimum transfer data melintasi jalur tertentu.
Ciphertext	Pesan yang sudah disembunyikan makna aslinya karena dienkripsi
DES	*Data Encryption Standard*, algoritma kunci simetris untuk enkripsi data elektronik
Diffie-Hellman	Metode pertukaran kunci enkripsi di ruang publik
DSA	*Digital Signature Algorithm*, algoritma untuk membuat tanda tangan digital
DSS	*Digital Signature Scheme*, teknik memastikan pengakuan suatu entitas karena telah melihat suatu pesan digital
ECC	*Elliptic Curve Cryptography*, algoritma kriptografi yang menggunakan kurva elliptika
ECDSA	*Elliptical Curve Digital Signature Algorithm*, algoritma pembuatan tanda tangan digital dengan menggunakan kurva elliptika
Heksadesimal	Heksadesinal adalah data sistem angka proporsional yang memiliki basis 16

Istilah	Arti
IM	*Instant Messaging* , sistem komunikasi berbasis komputer antara dua orang atau lebih yang bekerja secara langsung dan tersinkronisasi dalam suatu jaringan
Key Exchange	Teknik kriptografi untuk melakukan pertukaran kunci enkripsi
Kriptografi	Kriptografi adalah studi tentang teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentikasi entitas, dan autentikasi asal data
Kriptografi hibrida	Metode kriptografi yang menggabungkan algoritma kriptografi simetri dan algoritma kriptografi asimetri
Man in the Middle	Serangan dimana penyerang secara diam-diam mengubah komunikasi antara dua pihak yang yakin bahwa mereka berkomunikasi secara langsung satu sama lain.
RSA	*Riverse-Shamir-Adleman*, sistem kriptografi kunci publik yang banyak digunakan untuk transmisi data yang aman.
Throughput	Tingkat seberapa besar sesuatu diproses.

DAFTAR PUSTAKA

Abidi, A., Bouallegue, B., & Kahri, F. (2014). Implementation of elliptic curve digital signature algorithm (ECDSA). *GSCIT 2014 - Global Summit on Computer and Information Technology*, *June 2014*. https://doi.org/10.1109/GSCIT.2014.6970118

Alegro, J. K. P., Arboleda, E. R., Pereña, M. R., & Dellosa, R. M. (2019). Hybrid schnorr, rsa, and aes cryptosystem. *International Journal of Scientific and Technology Research*, *8*(10), 1770–1776.

Anand Kumar, M., & Karthikeyan, S. (2012). Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. *International Journal of Computer Network and Information Security*, *4*(2), 22–28. https://doi.org/10.5815/ijcnis.2012.02.04

Angrisani, L., Arpaia, P., Bonavolonta, F., & Cioffi, A. (2020). Experimental test of ECDSA digital signature robustness from timing-lattice attack. *I2MTC 2020 - International Instrumentation and Measurement Technology Conference, Proceedings*, 1–6. https://doi.org/10.1109/I2MTC43012.2020.9129144

Asiyanik. (2017). Studi Terhadap Advanced Encryption Standard (Aes) DanAlgoritma Knapsack Dalam Pengamanan Data. *Santika*, *7*(Jurnal Ilmiah Sains dan Teknologi), 553–561.

Atmojo, W. P., Isnanto, R. R., & Kridalukmana, R. (2016). Implementasi Aplikasi Kriptografi Pada Layanan Pesan Singkat (SMS) Menggunakan Algoritma RC6 Berbasis Android. *Jurnal Teknologi Dan Sistem Komputer*, *4*(3), 450. https://doi.org/10.14710/jtsiskom.4.3.2016.450-453

Bangalorekar, T. D., Panse, M. S., & Khandare, A. (2013). *Communication of Ionosonde system with a PC using LabVIEW for Hexadecimal data and comparison between Hexadecimal and ASCII modes*. *3*(1), 1690–1693.

Basri, B. (2018). Kriptografi Simetris dan Asimetris Dalam Perspe tif Keamanan Data dan Komple sitas Komputasi. *Jurnal Ilmu Komputer*, *2*(2), 17–23.

Bishop, M. (2004). *Introduction to Computer Security*. Prentice Hall PTR.

Coron, J.-S., Gutmann, E. P., Naccache, D., & Palmer, C. C. (2006). *What Is Cryptography?*

CORRESPONDENT, H. (2019, November). CERT-In asks users to update WhatsApp after MP4 video file vulnerability discovered. *Hindustant Times*. https://tech.hindustantimes.com/tech/news/cert-in-asks-users-to-update-whatsapp-after-mp4-video-file-vulnerability-discovered-story-Y4xBqsnttLDRvHIgCoEuuJ.html

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael. In *New York*. http://portal.acm.org/citation.cfm?id=560131

Delfs, H., & Knebl, H. (2007). *Information to Cryptography*.

Devi.T, R. (2013). Importance of cryptography in network security. *Proceedings - 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013*, 462–467. https://doi.org/10.1109/CSNT.2013.102

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*, 6. https://doi.org/10.1109/TIT.1976.1055638

EDUCBA. (2019). *Introduction to Digital Signature Algorithm*. https://www.educba.com/digital-signature-algorithm/

Enberg, J. (2019). *Global Messaging Apps 2019*. EMarketer.

Garg, N., & Yadav, P. (2014). Comparison of Asymmetric Algorithms in Cryptography. *IJCSMC*, *3*, 1190–1196.

Gupta, S., & Sharma, J. (2012). A hybrid encryption algorithm based on RSA and Diffie-Hellman. *2012 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2012*, 5–8. https://doi.org/10.1109/ICCIC.2012.6510190

Gutub, A. A. A., & Khan, F. A. A. (2012). Hybrid crypto hardware utilizing symmetric-key and public-key cryptosystems. *Proceedings - 2012 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2012*, 116–121. https://doi.org/10.1109/ACSAT.2012.44

Harkenson, D., Vanstone, S., & Menezes, A. (2004). *Guide to Elliptic Curve Cryptography*. Springer-Verlag. https://doi.org/10.1007/b97644

Harn, L., & Mehta, M. (2004). Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA). *IEEE Communications Letters*, *8*(3), 198–200. https://doi.org/10.1109/LCOMM.2004.825705

Hornsby, A., & Walsh, R. (2010). From Instant Messaging to Cloud Computing,

an XMPP revirw. *IEEE 14th International Symposium on Consumer Electronics*. https://doi.org/10.1109/ISCE.2010.5523293

Hutter, M., Feldhofer, M., & Wolkerstorfer, J. (2011). A cryptographic processor for low-resource devices: Canning ECDSA and AES like sardines. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6633 LNCS*, 144–159. https://doi.org/10.1007/978-3-642-21040-2_10

Indonesia, T. C. (2019). Keamanan WhatsApp Jadi Celah Sabotase Pesan. *CNN Indonesia*.

Iyer, S. C., Sedamkar, R. R., & Gupta, S. (2016). A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach. *Procedia Computer Science*, *79*, 293–298. https://doi.org/10.1016/j.procs.2016.03.038

Jain, M., & Agrawal, A. (2014). Implementation of hybrid cryptography algorithm. *International Journal Of Core Engineering & Management (IJCEM)*, *1*(3), 126–142.

Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36–63. https://doi.org/10.1007/s102070100002

Kartit, Z., Azougaghe, A., Idrissi, H. K., Marraki, M. El, Hedabou, M., Belkasmi, M., & Kartit, A. (n.d.). *Applying Encryption Algorithm for Data Security in Cloud Storage*. 141–154. https://doi.org/10.1007/978-981-287-990-5

Khalique, A., Singh, K., & Sood, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. *International Journal of Computer Applications*, *2*(2), 21–27. https://doi.org/10.5120/631-876

KOMINFO. (2017). *Survey Penggunaan Teknologi Informasi Tahun 2017*.

Latif, S., Qayyum, J., Lal, M., & Khan, F. (2011). Complete description of well-known number systems using single table. *International Journal of Electrical & Computer Sciences IJECS-IJENS*, *11*(3), 23–29. http://www.ijens.org/Vol 11 I 03/114403-5050 IJECS-IJENS.pdf

Levy, S. (2015). *Performance and Security of ECDSA*. Computer Science.

Liu, D. (2009). *Next Generation SSH2 Implementation*. Elsevier. https://doi.org/https://doi.org/10.1016/B978-1-59749-283-6.X0001-3

Logreira, R. C., Florez, Z. J., & Munoz, M. (2017). Cryptographic library performance comparison for instant messaging system centralized data.

Proceedings - International Carnahan Conference on Security Technology. https://doi.org/10.1109/CCST.2016.7815704

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology*, *13*(15).

Manel, D., Raouf, O., Ramzi, H., & Mtibaa, A. (2013). Hash function and Digital Signature based on elliptic curve. *14th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, STA 2013, February*, 388–392. https://doi.org/10.1109/STA.2013.6783160

Mathur, R., Agarwal, S., & Sharma, V. (2015). Solving security issues in mobile computing using cryptography techniques — A Survey. *International Conference on Computing, Communication & Automation*, 492–497. https://doi.org/10.1109/CCAA.2015.7148427

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*. CRC Press. https://doi.org/10.1201/9780429466335

Menezes, A., van Oorschot, P., & Vanstone, S. (1977). *Handbook of Applied Cryptography*.

Mondal, R., Ngo, H., Shey, J., Rakvic, R., Walker, O., & Brown, D. (2020). Efficient architecture design for the AES-128 algorithm on embedded systems. *17th ACM International Conference on Computing Frontiers 2020, CF 2020 - Proceedings*, 89–97. https://doi.org/10.1145/3387902.3392624

Munir, R. (2006). *Kriptografi*. Informatika.

Munir, Rinaldi. (2014). Algoritma Brute Force. *Www.Ilmuskripsi.Com*, 30. https://www.ilmuskripsi.com/2016/05/algoritma-brute-force.html

Nardi, B. A., Whittaker, S., & Bradner, E. (2000). *Interaction and Outeraction : Instant Messaging in Action*.

NIST, F. P. (2013). Digital Signature Standard (DSS). In *Safeguarding Critical E-Documents* (Issue July). https://doi.org/10.6028/NIST.FIPS.186-4

NIST, F. P., & PUBS.F. (2001). Advanced Encryption Standard (AES). *FIPS*, *197*(21). https://doi.org/10.6028/NIST.FIPS.197

Nti, I. K., Gymfi, E., & Nyarko, O. (2017). Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization. *International Journal of Advancements in Technology*, *08*(02), 1–5. https://doi.org/10.4172/0976-4860.1000183

P., P., N., P., R., M., N., K., & P., S. (2014). Comparative Analysis of DES, AES, RSA Encryption Algorithms. *International Journal of Engineering and Management Research (IJEMR)*, *4*(1), 132–134.

Pancholi, V. R., & Patel, B. P. (2016). Enhancement of Cloud Computing Security with Secure Data Storage using AES. *International Journal for Innovative Research in Science & Technology (IJIRST)*, *2*(09), 18–21.

Patil, P., Narayankar, P., Narayan D.G., & Meena S.M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617–624. https://doi.org/10.1016/j.procs.2016.02.108

Ramaraj, E., Karthikeyan, S., & Hemalatha, M. (2009). A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA). *International Journal of The Computer, the Internet and Management*, *17*(1), 78–86.

Rayarikar, R., Upadhyay, S., & Pimpale, P. (2012). SMS Encryption using AES Algorithm on Android. *International Journal of Computer Applications*, *50*(19), 12–17. https://doi.org/10.5120/7909-1038

Roy, A. (2016). Brief comparison of RSA and diffie-hellman (public key) algorithm. *ACCENTS Transactions on Information Security, Vol 1(1)*, *1*(1), 1–4.

Schneier, B. (2007). *Applied Cryptography*.

Sommerville, I. (2016). *Software Engineering 6TH Edition Synopses and Reviews Table of Contents*. 1–7.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices Fourth Edition*. Prentice Hall.

Sutrina, R. Y. (2016). *Sistem Autentikasi Pengunggahan File dengan Algoritma ECDSA*.

Thakur, J., & Kumar, N. (2011). *DES , AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis*. *1*(2), 6–12.

Vanstone, S. A. (1992). *Responses to NIST's Proposal*. *35*, 50–52.

Vijayakumar, R., Raja, S., & Prabakaran, M. (2014). ECDSA -Performance improvements of intrusion detection in Mobile Ad-hoc Networks.

Compusoft, *3*(1), 484–486.

Wijaya, A. (2015). *Sistem Enkripsi Menggunakan Algoritma Aes-128 Pada Prototype Community Messenger Berbasis Android Encryption System Using Aes-128 Algorithm on Prototype Community Messenger Android-Based*. *2*(2), 3306–3311.

Yahfizham, Y. (2019). *DASAR-DASAR KOMPUTER*.

You, W., Shi, G., Chen, X., Qi, J., & Qing, C. (2018). Research on a hybrid system with perfect forward secrecy. *Proceedings of the 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2017*, *2018-Janua*(1942), 1783–1787. https://doi.org/10.1109/ITNEC.2017.8285102